William F. Auther (014317)
Travis M. Wheeler (026415)
BOWMAN AND BROOKE LLP
Suite 1600, Phoenix Plaza
2901 North Central Avenue
Phoenix, Arizona 85012-2736
Telephone: (602) 643-2300
Fax: (602) 248-0947
William.Auther@bowmanandbrooke.com
Travis.Wheeler@bowmanandbrooke.com

John A. Vogt (*pro hac vice pending*)
Ryan D. Ball (*pro hac vice pending*)
JONES DAY
3161 Michelson Drive, Suite 800
Irvine, CA 92612
Telephone: 949.851.3939
Facsimile: 949.553.7539
javogt@jonesday.com
rball@jonesday.com

David M. Morrell (*pro hac vice forthcoming*)
JONES DAY
51 Louisiana Avenue, N.W.
Washington, D.C. 20001
Telephone: 202.879.3939
Facsimile: 202.626.1700
dmorrell@jonesday.com

Attorneys for Defendant HDR, Inc.

UNITED STATES DISTRICT COURT
DISTRICT OF ARIZONA

Carol Davis, individually and on behalf of all others similarly situated,

Plaintiff,

vs.

HDR, Inc.,

Defendant.

Case No. 2:21-cv-01903-SPL

DEFENDANT HDR, INC.'S MOTION TO DISMISS PLAINTIFF'S COMPLAINT; MEMORANDUM OF POINTS AND AUTHORITIES IN SUPPORT

(ORAL ARGUMENT REQUESTED)

///

///

///

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page(s)

CASES

INTRODUCTION

In this putative class action, Carol Davis claims that HDR, Inc. intercepted and accessed postings she allegedly made in two Facebook groups in violation of the federal Wiretap Act, the Stored Communications Act ("SCA"), and Arizona state invasion of privacy law. Her claims are meritless and cannot be cured with leave to amend.

First, none of her claims may move forward because her alleged postings on Facebook were not *private*—a threshold requirement to state a claim. While Ms. Davis alleges that the Facebook groups in which she posted content were nominally designated as "Private" groups, that label carries no legal weight, as entry into these groups, and the communications made within them, are readily accessible to the public. *See Snow v. DirecTV, Inc.*, 450 F.3d 1314, 1321 (11th Cir. 2006) (federal privacy claims dismissed even though the postings were made on a website styled as a "non-commercial private support group"). Indeed, the groups in which Ms. Davis allegedly posted content have thousands of members, and all communications made within those groups can freely be disseminated to others outside the groups. Ms. Davis never had any control over who joins the groups and thus who received her communications. Nor has she ever had control over the re-publication of her communications by group members to those outside the groups. To the contrary, Facebook informed Ms. Davis that any one of the thousands of recipients of her communications could "download, screenshot, or reshare [her] content to others" outside of Facebook. *See* Request for Judicial Notice ("RJN"), Ex. 1 at 6. As a matter of law, her communications were not private, which is fatal to her case.

Second, her claim under the federal Wiretap Act independently fails because a violation of that statute requires unlawful "interception" of a communication while it is still "in flight"—*i.e.*, *before* it appeared on Facebook. Ms. Davis does not plead any facts sufficient to establish a statutory violation, instead relying on generalized and conclusory allegations regarding

HDR's "STRATA" service.[1] But nothing about this service demonstrates that HDR unlawfully incepted communications in flight. Indeed, Ms. Davis pleads that it is "unknown" how or when HDR allegedly intercepted her communications, which means she cannot plausibly allege key elements of her Wiretap claim, including that HDR used unlawful means to obtain her postings. *See Quigley v. Yelp, Inc.*, No. 17-cv-3771, 2018 WL 7204066, at *4 (N.D. Cal. Jan. 22, 2018) (dismissing Wiretap Act where, as here, plaintiff did not "allege *with particularity* how or when any defendant became aware of his communications") (emphasis added).

Third, her claim that HDR violated the Wiretap Act by unlawfully possessing a wiretap device is even further afield. To start, Ms. Davis does not plead any facts establishing that HDR possessed a wiretap device. But even if she had alleged such facts, the Wiretap Act *criminalizes* the "manufacture[], assembl[y], possess[ion], or [sale]" of a wiretap device. *See* 18 U.S.C. § 2512(1)(b). It does not authorize a private cause of action for such conduct. Under the Act's remedial provisions, civil liability lies only where a person's communications are unlawfully "intercepted, disclosed, or intentionally used" by a wiretap device. *Id.* § 2520(a). Mere possession of a wiretap device is not enough. Or, as the Eleventh Circuit put it, "the plain language of section 2520(a) does not create a private right of action against a person who possesses a device in violation of section 2512(1)(b)." *DirecTV, Inc. v. Treworgy*, 373 F.3d 1124, 1125 (11th Cir. 2004).

Fourth, her claim under the SCA independently fails because, as noted, Ms. Davis admits that it is "unknown" how or when HDR allegedly intercepted her communications. Thus, she cannot plausibly allege key elements of her SCA claim, including that HDR accessed her communications "without authorization" while those communications were in "electronic

[1] Contrary to Ms. Davis' Orwellian allegations, there is nothing nefarious about reviewing communications from community members in a public forum concerning matters of public concern, such as government works projects. Rather, such practices are routinely conducted to assess public sentiment surrounding proposed projects, and address potential concerns of community members. Indeed, this is precisely what government officials (and their contractors) should do in evaluating proposed projects—*i.e.*, consider public sentiment around the project.

storage." Instead, she again relies only on conclusory and generalized allegations regarding HDR's purported misconduct. *See Russo v. Microsoft Corp.*, No. 20-cv-04818-YGR, 2021 WL 2688850, at *3 n.3 (N.D. Cal. June 30, 2021) ("The SCA provides a cause of action to a person 'aggrieved by any violation,' 18 U.S.C. § 2707(a), which typically requires a plaintiff to 'allege[] *with particularity* that her communications were part of the [disclosure].'" (emphasis added) (quoting *Jewel v. Nat'l Sec. Agency*, 673 F.3d 902, 910 (9th Cir. 2011)).

Fifth, Ms. Davis fails to allege the necessary elements of her common law invasion of privacy claim. This claim is grounded on her assertion that HDR intentionally intruded upon her conversations with members of the Facebook groups she joined. However, she fails to plead "an intentional intrusion into a private place, conversation, or matter." *Med. Lab'y Mgmt. Consultants v. Am. Broad. Cos.*, 306 F.3d 806, 812 (9th Cir. 2002) (applying Arizona law). Nor could she ever so allege. Any communications she posted are readily accessible to the public, and she has no ability to control who receives her postings and how those communications are disseminated to third parties outside the Facebook groups. Moreover, Ms. Davis was advised of her lack of control over communications when she signed up with Facebook, before she made any communications. She also does not identify any post she made, much less demonstrate that those posts involved her "private and personal affairs." *Id.* at 814. Ms. Davis thus cannot show that she had either a subjective expectation, or an objectively reasonable expectation, that her communications were or would remain private. Nor can she show that HDR's alleged intrusion into her communications was "highly offensive," as that requires a showing of "an exceptional kind of prying into another's private affairs." *Id.* at 819. Ms. Davis' posts were made to thousands of recipients, many of whom were undoubtedly strangers, and their substance did not implicate her "private affairs." Any intrusion into these communications, which HDR denies occurred, "was *de minimis* and thus not highly offensive to a reasonable person." *Id.*

In sum, Ms. Davis' Facebook postings were not private; her allegations of wrongdoing against HDR are so vague and conclusory that they could be filed against nearly any user of a social media platform; and her legal theories are so sweeping and broad that they effectively

would confer privacy rights over virtually any electronic communication. The Court should thus dismiss this action as a matter of law under Rule 12(b)(6).[2]

MEMORANDUM OF POINTS AND AUTHORITIES

SUMMARY OF ALLEGATIONS

HDR is an architecture and design firm with projects around the country. ECF No. 1 ("Compl.") at ¶ 12. In addition to its architectural services, HDR provides planning and consulting services, which include gauging public sentiment and developing media campaigns related to proposed or existing projects. *Id.* at ¶¶ 13–14. In August 2021, an article published in *Vice* claimed that in providing these services, HDR was "[s]pying" on Facebook groups run by activists opposed to particular HDR projects. *See id.* ¶ 29 & n.2. The article did not elaborate on how HDR allegedly "surveilled" these groups, but it did identify two allegedly affected groups by name—Ahwatukee411 and Protecting Arizona's Resources & Children ("PARC"). Based on this reporting (*id.*), Plaintiff Carol Davis, who belonged to both groups, filed this complaint. Her central allegation is that HDR "monitored" or "intercepted" her communications within these groups in violation of federal and state law.

Both Facebook groups were formed to enable those with an interest in the Ahwatukee community and members of the PARC organization to discuss local issues. *Id.* at ¶¶ 25, 27. Though nominally styled "private," both Facebook groups boast scores of members. Ahwatukee411, created in 2014, has more than 32,000 members, while PARC, created in 2016, has nearly 1,000. *Id.* at ¶¶ 24, 26.

To join the groups, interested Facebook users undergo a "screening process" allegedly intended to limit membership to local residents. *Id.* at ¶¶ 25, 27. The complaint does not describe the screening process for PARC, but claims that prospective members of Ahkwatukee411 must "fill out a questionnaire discussing their involvement in the Ahwatukee

[2] Pursuant to LRCiv 12.1(c), undersigned counsel hereby certifies that Defendant notified Plaintiff of the issues asserted in this motion, but the parties were unable to agree that the pleading was curable in any part through amendment. In fact, Ms. Davis' counsel stated that they saw no need to amend and could not identify any additional facts to allege.

community and their interest in joining the group." *Id.* at ¶ 25. Ms. Davis reports that she joined Ahwatukee411 in 2015 and PARC in 2016. *Id.* at ¶¶ 5–6, 35, 37, 39.

Ms. Davis alleges that she made numerous "posts" within these groups, including on topics such as recommendations for services, debates over political corruption, and the construction of a local highway, including its environmental impact. *Id.* at ¶¶ 5–6, 35–38. And she asserts that HDR "infiltrated, monitored, wiretapped, and/or accessed" posts within the groups since at least 2016. *Id.* at ¶ 29. Like the *Vice* article, however, Ms. Davis does not specify the manner or method by which HDR allegedly did so. She speculates that HDR may have used a "fake social media profile[]" or "some other method" to surveil the groups, but admits that the means are actually "unknown." *Id.* at ¶ 30. The complaint does not identify which posts HDR allegedly intercepted, when, or whether the posts reflected private or sensitive information.

Based upon these allegations, Ms. Davis asserts four claims on behalf of herself and two putative classes of members of the Facebook groups. She contends that HDR violated the federal Wiretap Act's prohibition on "intentionally intercept[ing] … any … electronic communication" through the use of a wiretap device, 18 U.S.C. § 2511 (Count I), as well as the Act's prohibition on "manufactur[ing], assembl[ing], [or] possess[ing]" a wiretap device, *id.* § 2512(1)(b) (Count II). She also alleges that HDR violated the Stored Communications Act ("SCA") by "access[ing]" group posts that were "in electronic storage," *id.* §§ 2701(a)(1), 2707(a) (Count III), and invaded her common law right to privacy by unlawfully accessing communications within the groups (Count IV).

LEGAL STANDARD

Federal Rule of Civil Procedure 12(b)(6) requires dismissal if a complaint either lacks "a cognizable legal theory or sufficient facts to support a cognizable legal theory." *Mendiondo v. Centinela Hosp. Med. Ctr.*, 521 F.3d 1097, 1104 (9th Cir. 2008). "To survive a motion to dismiss, a complaint must contain sufficient factual matter, accepted as true, to 'state a claim to relief that is plausible on its face.'" *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007)).

A claim is facially plausible when the factual allegations permit "the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Id.* Conclusory statements—such as mere "'labels and conclusions' or 'a formulaic recitation of the elements of a cause of action'"—do not suffice. *Id.* Instead, legitimate, non-conclusory factual allegations in the complaint "must be enough to raise a right to relief above the speculative level." *Twombly*, 550 U.S. at 555. This determination is context-specific, requiring a court to draw on its experience and common sense, but there is no plausibility "where the well-pleaded facts do not permit the court to infer more than the mere possibility of misconduct." *Iqbal*, 556 U.S. at 679.

When ruling on a motion to dismiss, the Court may consider the facts alleged in the complaint, documents attached to the complaint, documents relied upon but not attached to the complaint when authenticity is not contested, and matters of which the Court takes judicial notice. *Lee v. City of Los Angeles*, 250 F.3d 668, 688–89 (9th Cir. 2001).

LEGAL ARGUMENT

Ms. Davis' claims fail as a matter of law because the Facebook groups at issue are readily accessible to the public and she had no reasonable expectation that her communications would remain private. The groups comprised thousands of users, and were readily accessible to thousands more, who could gain access to anything Ms. Davis posted and further disseminate those communications outside the Facebook groups without limitation. She also had no control over who could join the groups and access posted content or the privacy setting of the groups. Her communications were, in short, not private and thus not protected. Moreover, her complaint fails to plausibly allege the essential elements of her claims, including, most glaringly, that HDR used *unlawful* (rather than lawful) means to allegedly obtain her communications.

I. Ms. Davis' Communications Were Not Private

Privacy is an essential element of Ms. Davis' claims. The Wiretap Act and the SCA foreclose liability where an intercepted communication "is readily accessible to the general public." 18 U.S.C. § 2511(2)(g)(i). This provision reflects Congress's goal in passing the

Electronic Communications Privacy Act ("ECPA")—which amended the Wiretap Act and created the SCA—"to afford privacy protection to electronic communications." *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 874 (9th Cir. 2002); *Snow*, 450 F.3d at 1320 ("The ECPA was enacted to … protect the privacy of the growing number of electronic communications."). Privacy is thus the touchstone for Wiretap Act and SCA claims. *See, e.g.*, *Ehling v. Monmouth-Ocean Hosp. Serv. Corp.*, 961 F. Supp. 2d 659, 668 (D.N.J. 2013) ("The touchstone of the [ECPA] is that it protects private information."); *Burke v. New Mexico*, No. 16-cv-0470, 2018 WL 3054674, at *5 (D.N.M. June 20, 2018) ("In the context of SCA claims, as with related Fourth Amendment claims, privacy is the touchstone."). A common law invasion of privacy claim similarly requires a reasonable expectation of privacy. *See Med. Lab'y Mgmt.*, 306 F.3d at 812–13.

In the eyes of the law, it is immaterial that the two Facebook groups in which Ms. Davis posted content were nominally designated "private." *See, e.g.*, *Snow*, 450 F.3d at 1321 (dismissing an SCA claim even though website was styled a "non-commercial private support group"); *Burke*, 2018 WL 3054674, at *8 (dismissing SCA claim where page access was restricted to registered website users). What matters is whether Ms. Davis' posts were "configured in some way so as to limit ready access by the general public." *Snow*, 450 F.3d at 1322; *see also Facebook, Inc. v. Superior Ct.*, 4 Cal. 5th 1245, 1270 (2018) ("[W]hen it comes to privacy protection, the critical inquiry is whether Facebook users took steps to limit access to the information [in their posts]."") (quoting *Ehling*, 961 F. Supp. 2d at 668). They were not, as Ms. Davis' allegations make clear.

To start, her communications were not meaningfully private because no private information was required to access them. Any member of the groups could view and disseminate her posts—and, to join the groups, prospective users did not have to enter usernames or passwords, or otherwise supply sensitive information. *See, e.g.*, *Burke*, 2018 WL 3054674, at *8 (dismissing SCA claim because complaint failed to allege "what private information Defendants were required to rely on, and did in fact rely on, in order to access [plaintiff's] website"). Rather, aspiring group members were asked to describe their

"community involvement" and "interest." Even if required by group administrators, such subjective self-disclosures, in response to a vague and open-ended prompt, is insufficient "to limit ready access by the general public," *see Snow*, 450 F.3d at 1322 (finding requirement that users affirm their non-association with particular companies insufficient for SCA claim), and nothing like the objective, verifiable, and non-public information that meaningfully limits the public's access to a website, *see Konop*, 302 F.3d at 872–73 (finding website private where, to gain access, user had to enter a name that appeared on a non-public access list created by website operator).

Moreover, even if joining the groups had been more restricted, Ms. Davis' communications within the groups still were not private. Administrators of the groups have unfettered discretion over access to group communications. Administrators can choose not to enforce the nominal requirements they have imposed by automatically granting requests to join the group. *See Republic of Gambia v. Facebook, Inc.*, No. 20-mc-36, 2021 WL 4304851, at *11 (D.D.C. Sept. 22, 2021), vacated in part on other grounds, 2021 WL 5758877 (D.D.C. Dec. 3, 2021) ("Administrators can automatically grant access to every requestor, such that a private group effectively becomes public."). Administrators can also "change the privacy of a Facebook group," RJN Ex. 2, or "the requirements for pending members to join [the] group at any time," RJN Ex. 3. A group member who is not an administrator has no control over the recipients of her communications or even the continuing designation of the groups as private.

Ms. Davis also had no control over the dissemination of her posts outside the groups themselves. As Facebook expressly informs its users, "when you share a post or send a message to specific friends or accounts, they can download, screenshot, or reshare that content to others across or off our Products, in person or in virtual reality experiences such as Facebook Spaces." RJN Ex. 1 at 6. Under these circumstances, the nominal designation of these groups as private, without more, cannot transform Ms. Davis' public communications into protected private utterances. *See Rosario v. Clark Cnty. Sch. Dist.*, No. 13-cv-362, 2013 WL 3679375, at *6 (D. Nev. July 3, 2013) (recognizing that "even with a private [Twitter] account, the user is still 'disseminat[ing] his postings and information to the public'"); *Tompkins v. Detroit*

Metro. Airport, 278 F.R.D. 387, 388 (E.D. Mich. 2012) ("[M]aterial posted on a 'private' Facebook page, that is accessible to a selected group of recipients but not available for viewing by the general public, is generally not privileged, nor is it protected by common law or civil law notions of privacy."); *cf. Konop*, 302 F.3d at 872–73 (finding website to be non-public where the plaintiff "controlled access to his website by requiring visitors to log in with a user name and password," "created a list of people … who were eligible to access the website," and "prohibited users from disclosing the website's contents to anyone else").

This is not a case where a Facebook user has "limited access to her Facebook wall to only her Facebook friends." *Ehling*, 961 F. Supp. 2d at 669 (finding such posts covered by the SCA). In that context, an individual Facebook user can control who her friends are and whether the wall remains accessible to only those friends. Here, by contrast, Ms. Davis controls neither membership in the groups at issue nor whether membership is even required to access group communications. Her communications are thus not private, which requires dismissal of her case.

II. Ms. Davis Does Not Plausibly Plead That HDR Unlawfully "Intercepted" Her Communications

In Count I, Ms. Davis contends that HDR "monitored" or "intercepted" her communications within the Facebook groups in violation of the Wiretap Act. Compl. at ¶¶ 5–6, 32, 41, 50–60. But she fails to offer any facts regarding the method or manner by which HDR did so. She speculates that HDR may have used a "fake social media profile[]" or "some other method," but admits that the actual means are "unknown." *Id.* at ¶ 30. But by failing to explain "how or when" HDR became aware of her communications, Ms. Davis has failed to meet her most basic pleading obligations for this claim. *See, e.g.*, *Quigley*, 2018 WL 7204066, at *4 (dismissing Wiretap Act where plaintiff did not "allege with particularity how or when any defendant became aware of his communications"); *Satchell v. Sonic Notify, Inc.*, 234 F. Supp. 3d 996, 1007 (N.D. Cal. 2017) (dismissing Wiretap Act interception claim where it could not be "discern[ed] the exact manner" in which defendants were "alleged to have 'acquired' the contents of" a communication).

Particular examples of this deficiency in her allegations abound. For instance, under the Wiretap Act, an unlawful "intercept[ion]" requires "acqui[sition] during transmission" (as opposed to while "in electronic storage"). *E.g.*, *Konop*, 302 F.3d at 878. That is, the interception must occur while the communication was still "in flight." *United States v. Steiger*, 318 F.3d 1039, 1048–50 (11th Cir. 2003) ("[A] contemporaneous interception—*i.e.*, an acquisition during 'flight'—is required to implicate the [Wiretap Act] with respect to electronic communications."); *Luis v. Zang*, 833 F.3d 619, 627–28 (6th Cir. 2016) ("Interception must thus occur contemporaneously with the transmission of the communication; it must, in other words, catch the communication 'in flight' before the communication comes to rest and ceases to be a communication."); *Fraser v. Nationwide Mut. Ins. Co.*, 352 F.3d 107, 113 (3d Cir. 2003) (same); *Steve Jackson Games, Inc. v. U.S. Secret Serv.*, 36 F.3d 457, 458 (5th Cir. 1994) (same).

Ms. Davis baldly asserts that the acquisitions were "in real time," but fails to offer any factual basis establishing that HDR intercepted her Facebook posts "in flight"—*i.e.*, *before* they appeared on the website. *See Crowley v. CyberSource Corp.*, 166 F. Supp. 2d 1263, 1269 (N.D. Cal. 2001) ("Crowley transmitted this information via e-mail over the Internet, and Amazon received the information, effectively completing the communication. Amazon did not, however, 'intercept' the communication within the meaning of the Wiretap Act, because Amazon did not acquire it using a device other than the drive or server on which the e-mail was received."). In short, there are no well-pleaded allegations establishing that HDR acquired any "communication" on Ms. Davis' part while it was "in flight." Thus, the claim fails. *See In re Vizio, Inc., Consumer Priv. Litig.*, 238 F. Supp. 3d 1204, 1228 (C.D. Cal. 2017) (dismissing Wiretap Act interception claim where plaintiffs made only conclusory and vague allegations that defendant intercepted their communication "during transmission" and "in real time").

Likewise, an unlawful "intercept[ion]" requires use of an "electronic, mechanical, or other device." 18 U.S.C. § 2510(4). But here, too, Ms. Davis fails to describe any device or apparatus HDR purportedly used to acquire her communications. She asserts that HDR uses

"commercial off-the-shelf tools" to achieve the goals of a service known as "STRATA" (Compl. ¶¶ 15–18), but courts have deemed such vague and conclusory allegations to be insufficient in this context. *See Rosenow v. Facebook, Inc.*, No. 19-cv-1297, 2020 WL 1984062, at *7 (S.D. Cal. Apr. 27, 2020) (dismissing as "conclusory" a Wiretap Act interception claim alleging that defendant "knowingly used an algorithm to intercept and scan Plaintiff's incoming chat messages for content during transit"); *Quigley*, 2018 WL 7204066, at *4 (dismissing Wiretap Act claim where complaint made "vague references to 'surveillance systems' and 'surveillance personnel,'" but did not "allege with particularity how or when any defendant became aware of his communications").

Ms. Davis' bare-bones allegations also fail to establish that any acquisition of her communications was *unlawful*, which is particularly problematic given the obvious, lawful means by which HDR could have acquired them. For example, if an HDR employee had been a member of the groups—and was thus a party to the communications—there would be no unlawful "interception," since that occurs only when someone captures a communication "to *another* party." *Marsh v. Zaazoom Sols., LLC*, No. 11-cv-5226, 2012 WL 952226, at *17 (N.D. Cal. Mar. 20, 2012) (emphasis in original). In other words, as an "intended recipient" of, or "second party" to, the communication, the HDR employee would not have violated the Wiretap Act by acquiring the messages. *See id.* (quoting *Crowley*, 166 F. Supp. 2d at 1269); *accord Yunker v. Pandora Media, Inc.*, No. 11-cv-3113, 2013 WL 1282980, at *7–8 (N.D. Cal. Mar. 26, 2013); *Conte v. Newsday, Inc.*, 703 F. Supp. 2d 126, 140 (E.D.N.Y. 2010). The same would be true if HDR received consent to access the communications from any one of the groups' 33,000 members. *See* 18 U.S.C. § 2511(2)(d) (interception is lawful where "one of the parties to the communication has given prior consent to such interception"). As it is, Ms. Davis' complaint offers no basis to "infer more than the mere possibility of misconduct." *Iqbal*, 556 U.S. at 679.

Nothing in the *Vice* article compensates for the legal deficiency of her allegations. Like Ms. Davis' complaint, the *Vice* article makes vague assertions regarding "surveillance," but fails to detail how or when HDR purportedly intercepted the communications at issue. *See*

RJN Ex. 4. Her reliance on the *Vice* article thus cannot save her claim. *See Lopez v. Apple, Inc.*, 519 F. Supp. 3d 672, 681 (N.D. Cal. 2021) (dismissing claims where plaintiffs alleged in "conclusory fashion[] that their communications were intercepted and disclosed," and the complaint made clear the allegations were "based entirely on [a] *Guardian* article"). Count I must therefore be dismissed.

III. There Is No Private Right Of Action Over The Unlawful Possession Of A Wiretap Device

In Count II, Ms. Davis alleges that HDR unlawfully possessed a wiretap device. Compl. at ¶¶ 61–70. The claim is baseless. To start, she does not even adequately plead that HDR possessed a wiretap device. But even if she had, the Wiretap Act does not authorize a private cause of action for such conduct. Rather, the Act *criminalizes* the "manufacture[], assembl[y], possess[ion], or [sale]" of a wiretap device. 18 U.S.C. § 2512(1)(b). Civil liability lies only where a person's communications are unlawfully "intercepted, disclosed, or intentionally used" by a wiretap device. *Id.* § 2520(a). Mere possession of such a device is not enough. As several circuit courts have held, "the plain language of section 2520(a) does not create a private right of action against a person who possesses a device in violation of section 2512(1)(b)." *Treworgy*, 373 F.3d at 1125; *see also DIRECTV Inc. v. Robson*, 420 F.3d 532, 539 (5th Cir. 2005) ("Tellingly, however, the civil cause of action embodied in § 2520 does not cover [§ 2512] possessory violations."); *DIRECTV Inc. v. Nicholas*, 403 F.3d 223, 227 (4th Cir. 2005) (finding that the "express language of § 2520 is … not susceptible to a construction which would provide a cause of action against one who manufactures or sells a device in violation of § 2512 but does not engage in conduct violative of § 2511").

Although the Ninth Circuit has not itself squarely addressed this issue, it has cited the Eleventh Circuit's holding in *Treworgy* approvingly. *See DirecTV, Inc. v. Webb*, 545 F.3d 837, 844 (9th Cir. 2008). And numerous district courts—including within the District of Arizona—have adopted *Treworgy*'s holding. *See, e.g.*, *Yoon v. Lululemon USA, Inc.*, No. 20-cv-2439, 2021 WL 3615907, at *8 (C.D. Cal. July 15, 2021) ("[T]here is no private right of action for the violation of § 2512(1) of the Wiretap Act."); *In re Cases Filed by DIRECTV,*

Inc., 344 F. Supp. 2d 636, 646 (D. Ariz. 2004) ("the *Treworgy* decision provides important guidance" and "correctly interprets § 2512(1)(b)" to foreclose "a private cause of action based upon possession of a prohibited device"); *In re Lenovo Adware Litig.*, No. 15-md-2624, 2016 WL 6277245, at *7 (N.D. Cal. Oct. 27, 2016) ("Section 2512 … does not establish a private right of action—it addresses only criminal liability.").

This weight of authority is correct. By expressly granting a private right of action to "any person whose … electronic communication is intercepted," and further specifying the available remedies, defenses, and time limits on such claims, the omission of any reference to mere *possession* of a wiretap device confirms that the Act does not support a private right of action for violations of section 2512(1). *See* 18 U.S.C. § 2520. Count II of the complaint thus fails as a matter of law.

IV. Ms. Davis Fails To Plead A Violation Of The SCA

In Count III, Ms. Davis alleges that HDR violated the SCA by accessing her communications in the Facebook groups "without authorization" and while those communications were in electronic storage. *See* Compl. at ¶¶ 71–80. But, like her other claims, Count III contains nothing more than conclusory and generalized allegations regarding HDR's purported misconduct. Ms. Davis does not identify the means or method by which HDR purportedly accessed communications, or even whether HDR accessed any of her communications. She also fails to offer any facts supporting her allegation that HDR acted "without authorization," 18 U.S.C. § 2701(a)(1), which is particularly problematic given the lawful means available to access the communications at issue, *supra*, 12. These deficiencies are fatal to her claims. *See also Nexsales Corp. v. Salebuild, Inc.*, No. 11-cv-3915, 2012 WL 216260, at *3 (N.D. Cal. Jan. 24, 2012) (holding that "conclusory allegations do not support a claim under the Stored Communications Act"); *Russo*, 2021 WL 2688850, at *3 n.3 ("The SCA provides a cause of action to a person 'aggrieved by any violation,' 18 U.S.C. § 2707(a), which typically requires a plaintiff to 'allege[] with particularity that her communications were part of the [disclosure].'").

V. Ms. Davis Fails To Plead A Common Law Invasion Of Privacy Claim

Count IV alleges that HDR violated Ms. Davis' common law right to privacy by intentionally intruding upon her conversations with members of the Facebook groups. *See* Compl. at ¶¶ 81–92. But her allegations fail to plead either element of such a claim.

First, she fails to establish "an intentional intrusion into a private place, conversation, or matter." *Med. Lab'y Mgmt.*, 306 F.3d at 812. This element requires a plaintiff to show "(a) an actual, subjective expectation of seclusion or solitude in the place, conversation, or matter, and (b) that the expectation was objectively reasonable." *Id.* at 812–13. Ms. Davis makes no such showing here. As noted, her alleged communications are readily accessible to the public, and she alleges no ability to control membership in—or access to content posted in—the Facebook groups, let alone control the dissemination of her communications to third parties outside the Facebook groups. Indeed, Facebook's terms of service put Ms. Davis on notice of each of these facts. *See supra*, 9. She also fails to describe any particular posts she made, much less demonstrate that they involved her "private and personal affairs." *Med. Lab'y Mgmt*, 306 F.3d at 814. Thus, Ms. Davis fails to allege facts suggesting that she had either a subjective expectation, or an objectively reasonable expectation, that her communications were or would remain private. *See, e.g.*, *Heldt v. Guardian Life Ins. Co. of Am.*, No. 16-cv-885, 2019 WL 651503, at *7 (S.D. Cal. Feb. 15, 2019); *Tompkins*, 278 F.R.D. at 388; *United States v. Meregildo*, 883 F. Supp. 2d 523, 526 (S.D.N.Y. 2012).

Nor can she show that HDR's purported intrusion into her communications was "highly offensive," a second element of this claim. *Med. Lab'y Mgmt.*, 306 F.3d at 812. This prong requires "an exceptional kind of prying into another's private affairs." *Id.* at 819. Ms. Davis' posts were made to thousands of recipients, many of whom were undoubtedly strangers, and did not implicate her "private affairs." Instead, the posts addressed matters of public concern, such as debates over political corruption and the construction of a local highway, including its environmental impact. Compl. at ¶¶ 5–6, 35–38. Any intrusion into these types of communications would be "*de minimis* and thus not highly offensive to a reasonable person." *Med. Lab'y Mgmt.*, 306 F.3d at 819 ("The covert videotaping of a business conversation

among strangers in business offices does not rise to the level of an exceptional prying into another's private affairs, which … is required for 'offensiveness.'"); *Interscope Recs. v. Duty*, No. 05-cv-3744, 2006 WL 988086, at *3 (D. Ariz. Apr. 14, 2006) (dismissing intrusion upon seclusion claim where plaintiff alleged that defendant unlawfully accessed a publicly available share folder).

For these reasons, the common law invasion of privacy claim fails, and should be dismissed.

CONCLUSION

A court may dismiss a claim without leave to amend if the defects in the complaint cannot be cured by alleging additional facts. *See Lopez v. Smith*, 203 F.3d 1122, 1130 (9th Cir. 2000); *DeSoto v. Yellow Freight Sys. Inc.*, 957 F.2d 655, 658 (9th Cir. 1992). In other words, "futile amendments should not be permitted." *Klamath-Lake Pharm. Ass'n v. Klamath Med. Serv. Bureau*, 701 F.2d 1276, 1293 (9th Cir. 1983) (citing *Foman v. Davis*, 371 U.S. 178, 182 (1962)). Here, Ms. Davis cannot allege any additional facts to show that her posts—which were made to thousands of Facebook members—were private. Indeed, her own allegations demonstrate that her communications were not private, and that she could not have had a reasonable expectation otherwise. And, during the parties' meet and confer efforts, Ms. Davis' counsel could not identify any additional facts that could be alleged to substantiate her claims. Thus, there is "no need to prolong the litigation by permitting further amendment." *Lipton v. Pathogenesis Corp.*, 284 F.3d 1027, 1039 (9th Cir. 2002). The Court should dismiss this action with prejudice.

Dated this 14th day of January, 2022

BOWMAN AND BROOKE LLP

By: */s/William F. Auther*
William F. Auther
Travis M. Wheeler
Suite 1600, Phoenix Plaza
2901 North Central Avenue
Phoenix, Arizona 85012-2736

///

John A. Vogt (*pro hac vice pending*)
Ryan D. Ball (*pro hac vice pending*)
JONES DAY
3161 Michelson Drive, Suite 800
Irvine, CA 92612
Telephone: 949.851.3939
Facsimile: 949.553.7539
javogt@jonesday.com
rball@jonesday.com

David M. Morrell (*pro hac vice forthcoming*)
JONES DAY
51 Louisiana Avenue, N.W.
Washington, D.C. 20001
Telephone: 202.879.3939
Facsimile: 202.626.1700
dmorrell@jonesday.com

Attorneys for Defendant HDR, Inc.

CERTIFICATE OF SERVICE

I hereby certify that on January 14, 2022, I electronically transmitted the foregoing **DEFENDANT HDR, INC.'S MOTION TO DISMISS PLAINTIFF'S COMPLAINT; MEMORANDUM OF POINTS AND AUTHORITIES IN SUPPORT (ORAL ARGUMENT REQUESTED)** to the Clerk's Office using the CM/ECF System for filing and transmittal of a Notice of Electronic Filing to the following CM/ECF Registrants:

Gerald Barrett, SBN: 005855
WARD, KEENAN & BARRETT, P.C.
3838 N. Central Avenue, Suite 1720
Phoenix, Arizona 85012
Tel: (602) 279-1717
Fax: (602) 279-8908
E-Mail: gbarrett@wardkeenanbarrett.com

Neal J. Deckant
BURSOR & FISHER, P.A.
1990 North California Boulevard, Suite 940
Walnut Creek, CA 94596
Telephone: (925) 300-4455
Facsimile: (925) 407-2700
E-Mail: ndeckant@bursor.com

Joshua D. Arisohn
Alec M. Lesli
Max S. Roberts
BURSOR & FISHER, P.A.
888 Seventh Avenue
New York, NY 10019
Telephone: (646) 837-7150
Facsimile: (212) 989-9163
E-Mail: jarisohn@bursor.com
aleslie@bursor.com
mroberts@bursor.com

Attorneys for Plaintiffs

/s/Jeannette Felix